

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平9-245230

(43) 公開日 平成9年(1997)9月19日

(51) Int.Cl. ⁸	識別記号	庁内整理番号	F I	技術表示箇所
G 0 7 F 7/08			G 0 7 F 7/08	G
			G 0 7 G 1/14	
G 0 7 G 1/14			G 0 7 F 7/08	C

審査請求 未請求 請求項の数6 F D (全 7 頁)

(21) 出願番号 特願平8-73092

(22) 出願日 平成8年(1996)3月5日

(71) 出願人 595108206

株式会社アイネス

神奈川県横浜市都筑区牛久保3-9-2

(72) 発明者 小勝 康弘

神奈川県横浜市都筑区牛久保3-9-2

株式会社アイネス内

(72) 発明者 峯下 恒美

神奈川県横浜市都筑区牛久保3-9-2

株式会社アイネス内

(72) 発明者 鈴木 文史朗

神奈川県横浜市都筑区牛久保3-9-2

株式会社アイネス内

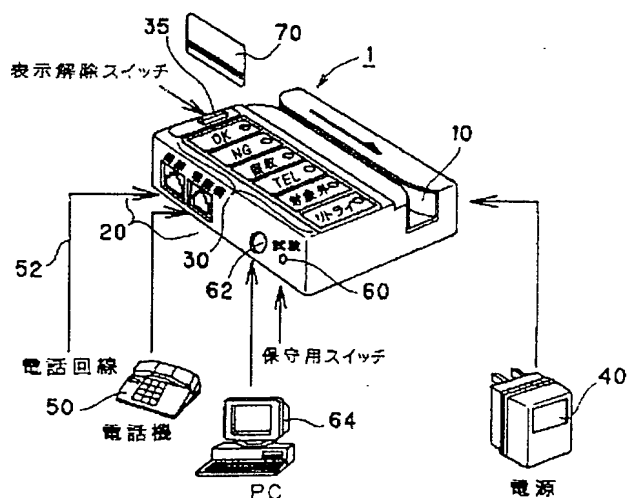
(74) 代理人 弁理士 的場 基憲

(54) 【発明の名称】 無効カードチェック装置及び無効カードチェックシステム

(57) 【要約】

【課題】 無効カードを迅速、簡易且つ低コストでチェックでき、不正なクレジット取引を防止できる無効カードチェック装置及び無効カードチェックシステムを提供する。

【解決手段】 チェック装置1は、クレジットカード70からカードデータを読み取るカードリーダー10と、N C U / モデム20と、表示ランプ30とを備える。モデム20には電話機50が接続され、公衆電話回線52を介してホストコンピュータと接続されている。チェックシステムは、チェック装置1と、ネットワーク80と、ホストコンピュータ90とを有する。



【特許請求の範囲】

【請求項1】 クレジット取引に際し、使用されるカードが無効カードか否かをチェックする装置であって、上記カードからカードデータを読み取る読取手段と、このカードデータを無効カードか否かの判定を行うホスト装置に送信し、且つこのホスト装置からの判定結果データを受信する伝送手段と、上記判定結果を表示する表示手段と、を備えることを特徴とする無効カードチェック装置。

【請求項2】 上記伝送手段が無線通信機を備えることを特徴とする請求項1記載の無効カードチェック装置。

【請求項3】 請求項1又は2記載の無効カードチェック装置と、この無効カードチェック装置とネットワークを介して接続されたホスト装置とを備え、上記ホスト装置は、上記無効カードチェック装置からのカードデータを無効カードデータと対比することにより、無効カードか否かの判定を行い、その判定結果データを上記無効カードチェック装置に伝送する、ことを特徴とする無効カードチェックシステム。

【請求項4】 上記ネットワークが上記無効カードチェック装置に対して複数個のアクセスポイントを有し、上記無効カードチェック装置が、これらアクセスポイントのうちの任意1箇所を優先的に指定する情報を格納したメモリを有することを特徴とする請求項3記載の無効カードチェックシステム。

【請求項5】 上記ネットワークが上記無効カードチェック装置に対して複数個のアクセスポイントを有し、且つ上記ホスト装置がアクセスポイントの変更情報を有し、

上記いずれかのアクセスポイントを介して、上記無効カードチェック装置から上記ホスト装置にデータ伝送があったとき、このホスト装置が上記変更情報に応じた変更信号を上記無効カードチェック装置に伝送し、この無効カードチェック装置のメモリに格納されているアクセスポイントの指定情報を書き換える、ことを特徴とする請求項3記載の無効カードチェックシステム。

【請求項6】 上記ネットワークに接続されたコンピュータ装置を備え、このコンピュータ装置が、アクセスポイントの変更情報を有し、且つこのアドレス変更情報に応じた変更信号を上記無効カードチェック装置に伝送し、この無効カードチェック装置のメモリに格納されたアクセスポイントの指定情報を書き換える、ことを特徴とする請求項3記載の無効カードチェックシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、無効カードチェック装置及びこれを用いた無効カードチェックシステムに係り、更に詳細には、クレジット取引に際し、使用されるクレジットカードが無効カードか否かを判定する装置及びシステムに関する。

【0002】

【従来の技術】 現在、クレジットカードを利用した取引が著しく普及している。かかるクレジット取引では、取引時に代金を支払う必要がなく、その後に所定の銀行口座などから取引代金を引き落とすので、多重債務者であっても取引が成立してしまうという問題がしばしば発生している。また、クレジット取引においては、通常、クレジットカードとサインにより本人か否かを判断するが、サインの同一性判断は困難なことが多いので、本人がクレジットカードを紛失し又は盗難された場合には、他人がそのクレジットカードを使用して不正な取引を行ったり、更には、盗難等による場合でなくとも、クレジットカード自体を偽造して不正な取引を行うという問題も発生している。

【0003】 このような問題に対し、各クレジット会社は、従来から、「無効カード通知書」という書類を作成して、多重債務、紛失、盗難及び偽造などに係るクレジットカード（以下、「無効カード」という）のカード番号をリストアップし、この書類を加盟店に郵送して注意を喚起することにより、多重債務、紛失、盗難及び偽造などによる不正なクレジット取引を防止しようとしている。また、一部の大規模加盟店などでは、信用照会端末（CAT; Credit Authorization Terminal）を導入し、クレジット取引の際には、クレジットカードのカード番号、支払い金額及び支払い方法などを、所定のネットワークを介してクレジット会社のホストコンピュータに伝送して照会することにより、かかる不正なクレジット取引を防止しようとしていた。

【0004】

【発明が解決しようとする課題】 しかしながら、このような従来の方法において、無効カード通知書による手法では、無効カード通知書に全ての無効カードがリストアップされている訳ではなく、リストから漏れた無効カードについては上述のような不正取引を防止できないという課題があった。また、無効カード通知書は、通常、毎月2回程度郵送されるにすぎないため、盗難などに係る無効カードが迅速にリストアップされることは少なく、迅速性に欠けるため、盗難後短期間による不正取引を防止し得ないという課題もある。更に、無効カード通知書は、通常、十数頁から成り、その頁毎に十数桁の無効カード番号が多数リストアップされているものであるため、加盟店ではカード番号の照合が困難であり、あまり利用されていないのが実状である。

【0005】 一方、CATを用いる手法では、クレジット取引時にホストコンピュータとの照会を行うため、販売時点情報管理（POS: Point Of Sale）を実現し、上述のような不正取引を有効に防止できるが、装置全体が大型で高価であるという課題があり、この結果、CATの普及率はクレジット加盟店全体の約

数%に過ぎなかった。本発明は、このような従来技術の有する課題に鑑みてなされたものであり、その目的とするところは、無効カードを迅速、簡易且つ低コストでチェックでき、不正なクレジット取引を防止できる無効カードチェック装置及び無効カードチェックシステムを提供することにある。

【0006】

【課題を解決するための手段】本発明者らは、上記目的を達成すべく鋭意検討した結果、CATを用いる手法で行う照会は、支払い金額を計算したり支払い方法を決定する決済をも含むものであるため、CAT自体として、10 支払い金額等を入力する手段やこれに用いるディスプレイ等を必要とするので、装置全体が大型化し易く、しかもコスト高となっていることを知見した。そして、かかる知見に基づき、本発明者らが更に検討を重ねた結果、ホスト装置との間で無効カードデータの照会のみを行い、決済を行わない構成とすることにより、上記目的が達成できることを見出し、本発明を完成するに至った。

【0007】即ち、本発明の無効カードチェック装置は、クレジット取引に際し、使用されるカードが無効カードか否かをチェックする装置であって、上記カードからカードデータを読み取る読取手段と、このカードデータを無効カードか否かの判定を行うホスト装置に送信し、且つこのホスト装置から判定結果データを受信する伝送手段と、上記判定結果を表示する表示手段とを備えることを特徴とする。また、本発明の無効カードチェックシステムは、上述の無効カードチェック装置と、この無効カードチェック装置とネットワークを介して接続されたホスト装置とを備え、上記ホスト装置は、上記無効カードチェック装置からのカードデータを無効カードデータと対比することにより、無効カードか否かの判定を行い、その判定結果を上記無効カードチェック装置に伝送することを特徴とする。

【0008】

【作用】本発明の無効カードチェックシステムにおいては、取引の際に使用されるクレジットカードが無効カードに該当するか否かを、無効カードデータを有するホスト装置と無効カードチェック装置との間でデータ通信することにより判定する。従って、使用されるクレジットカードが無効カードに該当するか否かを取引の時点で迅速に判定できる。また、ホスト装置の無効カードデータを更新すれば、無効カードに該当するか否かを、更新された無効カードデータに基づき更新時点から行うことができるので、クレジットカードが盗難されたような場合であっても、迅速な対処が可能である。

【0009】また、本発明の無効カードチェック装置では、取引の際に支払い代金の計算や支払い方法の決定を行わない。従って、このような決済機能が不要なため、金額入力手段や計算手段が不要であり、小型化及び低コスト化を図ることができる。

【0010】

【発明の実施の形態】以下、本発明を図面を参照して実施形態により詳細に説明するが、本発明はこれら実施形態に限定されるものではない。図1は、本発明の無効カードチェック装置の一実施形態を示す斜視図である。同図において、このチェック装置1は、クレジットカード70からカード番号や支払い指定口座番号などのカードデータを読み取る読取手段の一例であるカードリーダー10と、図示しないホストコンピュータとの間でデータ伝送を行う伝送手段の一例であるNCU/モデム20と、ホストコンピュータからの判定結果を表示する表示手段の一例である表示ランプ30とを備えており、図中40は電源を示している。

【0011】また、上記モデム20には電話機50が接続されており、これにより、チェック装置1は、公衆電話回線52を利用したネットワーク（図示せず）を介してホストコンピュータ（図示せず）と接続されている。更に、上記表示ランプ30は、OK、NG、…、対象外及びリトライランプに分割されており、これらランプは、ホストコンピュータからの判定結果に応じて点灯することができる。なお、図中、60は保守用スイッチであり、チェック装置1は、保守用インターフェイス部62を介してパーソナルコンピュータ64と接続可能な構成となっている。

【0012】図2は、図1に示した無効カードチェック装置1の電氣的構成を示す概略ブロック図である。同図において、制御部5は、図示しないCPUと、ROM及びRAMから成るメモリとを有し、ROMには、後述する図4のようなフローチャートに基づくCPUの動作プログラムが格納され、RAMには、カードデータやホストコンピュータからの判定結果データなどが格納される。なお、ブザー12は、クレジットカード70をカードリーダー10でスキャンした時に読み取り確認音を発生するものである。

【0013】図3は、本発明の無効カードチェックシステムの一実施形態を示す概略構成図である。同図において、このチェックシステムは、上述の無効カードチェック装置1と、電話回線52を利用したネットワーク80と、ホストコンピュータ90とを有し、加盟点に設置された無効カードチェック装置1は、ネットワーク80を介してホストコンピュータ90との間でデータ通信が可能に接続されている。なお、上述のネットワーク80は、無効カードチェック装置1に対して複数個のアクセスポイントAP1、AP2、…、APNを有している。また、ホストコンピュータ90は、適当な回線54、56及び58を介して各クレジット会社100、102のホストコンピュータ等と接続されており、ホスト90の無効カードデータは、各クレジット会社のホストコンピュータ等との間でデータ通信を行うことにより、50

迅速な更新が可能である。

【0014】次に、本実施形態の無効カードチェック装置及び無効カードチェックシステムの処理動作について説明する。図4は、本実施形態の無効カードチェックシステムの処理手順を示すフローチャートである。まず、クレジットカード70を無効カードチェック装置のカードリーダ10でスキャンさせ、カードデータを読み込む（ステップS1：以下、単に「S1」とする）（図1参照）。この読み込みが終了すると、ブザー12が読み取り確認音を発生し、ネットワーク80のアクセスポイントAP1へ自動的にダイヤリングが行われる（S2）（図3参照）。

【0015】この際、AP1に接続されない場合は、他のアクセスポイントAP2へダイヤリングが行われ（S3）、それでも接続されない場合には、無効カードチェック装置1の表示ランプ30の1つであるリトライランプが点灯し、再度処理を開始する必要がある旨が表示される。なお、本実施形態において、無効カードチェック装置1のROMには、ダイヤリング先として、AP1及びAP2がその電話番号とともに書き込まれており、また、ダイヤリングの優先順位はAP1>AP2となっている。一方、上記ダイヤリングにより所定のアクセスポイントとの接続が完了すると、上述のように読み込まれたカード番号、支払い口座番号等のカードデータがホストコンピュータ90に送信される（S4）（図3参照）。

【0016】次に、ホストコンピュータ90は、受信したカードデータを無効カードデータベースに蓄積されている無効カードデータと照会し、当該カードが取引可能なカードか無効カードであるか判定し、得られた判定結果データを無効カードチェック装置1に送信する。そして、無効カードチェック装置1がこの判定結果データを受信すると、電話回線が切断され（S5）、受信した判定結果データに応じて、表示ランプ30のいずれかのランプが点灯する。但し、判定結果データが所定時間内に受信されない場合には、無効カードチェック装置1のリトライランプが点灯することになっている。

【0017】ここで、本実施形態における上記判定結果データの内容を説明すると、無効カードに該当せず取引可能なカードである場合には、ホストコンピュータ90から「OK信号」が送信される。また、カードが、多重債務、限度額や有効期限の点で不適当であり無効カードに該当する場合には「NG信号」、紛失や盗難に係るものである場合には「回収信号」、クレジット会社間い合わせの場合には「TEL信号」、加盟店で取り扱っていないカードの場合には「対象外信号」、システム障害その他の場合には「リトライ信号」が送信される。そして、このような各種信号に応じて、無効カードチェック装置1の「NG」、「OK」、「回収」、「TEL」及び「対象外」ランプが点灯し、不正取引の防止に供され

る。

【0018】なお、上記NG信号の原因の1つである限度額については、対象となるカードによって予め定められている一定の取引可能金額（フロアリミット）であり、本実施形態では、このフロアリミットを超えるか否かが単純に判定される。従って、CATシステムのように、カード使用時点（取引時点）で購入した商品の代金をも考慮（計算）して限度額を超えるか否かを判定するものではない。

【0019】次に、本実施形態の無効カードチェックシステムにおけるアクセスポイントの変更（自動変更）について説明する。上述のように、無効カードチェック装置1において、アクセスポイントの指定は、通常、初期インストール時にROMにAP1及びAP2の電話番号を書き込むことによって行われている。このような状態において、後にネットワーク80が拡充されてアクセスポイントが増設されると、無効カードチェック装置1に対し、初期に指定されたアクセスポイント（AP1及びAP2）より近接するアクセスポイントAP3（図5参照）が出現する場合がある。

【0020】このような場合、本実施形態においては、図5に示すように、ホストコンピュータ90にアクセスポイントのアドレス変更情報（本例では、AP1の電話番号をAP3の電話番号に書き換える旨の指令）を付与し、AP1を介して無効カードチェック装置1からデータ伝送があったときには、ホストコンピュータ90がアドレス変更信号を無効カードチェック装置1に送信し、無効カードチェック装置1のROMに書き込まれているAP1の電話番号をAP3の電話番号に書き換えることができる。

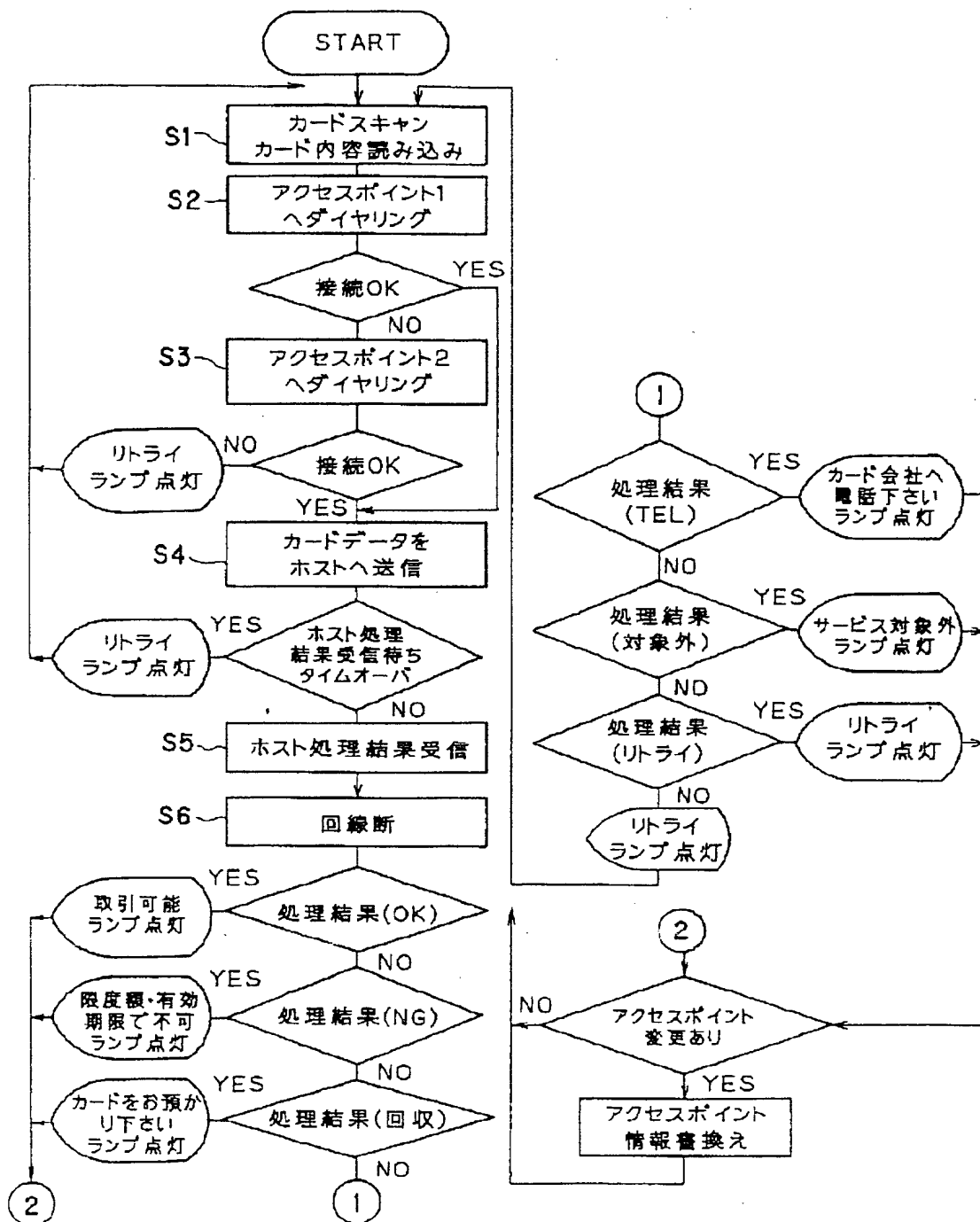
【0021】通常、アクセスポイントの変更は、無効カードチェック装置1側でROMを書き換えて行う必要があるが、この手法によれば、ホストコンピュータ90側からの処理によりアクセスポイントの変更を行うことができ、便利である。また、アクセスポイント変更の必要性は、上述のようにネットワーク80の拡充によって生ずるが、これ以外にも、災害などによって一定エリアのアクセスポイントが使用不能になったような場合にも生じ、かかる災害時に無効カードチェック装置1側での処理を必要とせず、アクセスポイントを変更できることは極めて便利である。

【0022】図6に、アクセスポイント変更方法の他の例を示す。同図において、パーソナルコンピュータ（以下、「PC」）92は、ネットワーク80に接続されており、アクセスポイントのアドレス変更情報を有する。このような場合、PC92から無効カードチェック装置1にアドレス変更情報を送信し、上記同様にAP1の電話番号をAP3の電話番号に書き換えることができる。

【0023】以上、本発明を実施形態により説明したが、本発明はこれら実施形態に限定されるものではない

20

【図4】



【図6】

